The New York Times Magazine

The Eroded Self

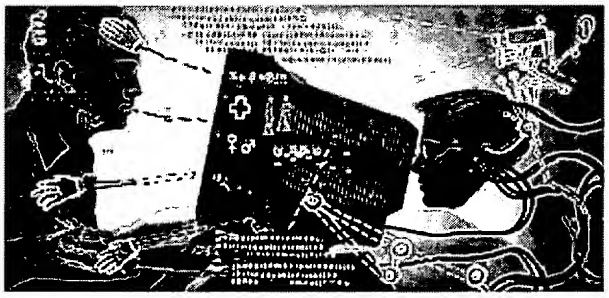
In cyberspace, there is no real wall between public and private. And the version of you being constructed out there - from bits and pieces of stray data - is probably not who you think you are.

By JEFFREY ROSEN Photographs by ANDREW ECCLES Illustrations by JONATHON ROSEN

Related Articles

- In Technology: Privacy in the Digital Age
- Prologue: The Unwanted Gaze: The Destruction of Privacy in America

---



Monica Lewinsky is a most unlikely spokesperson for the virtues of reticence. But in addition to selling designer handbags, she has emerged after her internship as an advocate of privacy in cyberspace. "People need to realize that your e-mails can be read and made public, and that you need to be cautious," she warned recently on "Larry King Live." Lewinsky was unsettled by Kenneth Starr's decision to subpoena Washington bookstores for receipts of her purchases; in her underappreciated biography, "Monica's Story," she points to the bookstore subpoenas as one of the most invasive moments in the Starr investigation. But she was also distraught when the prosecutors subpoenaed her home computer. From the recesses of her hard drive, they retrieved e-mail messages that she had tried unsuccessfully to delete, along with the love letters she had drafted -- but never sent -- to the president. "It was such a violation," Lewinsky complained to her biographer, Andrew Morton.

Many Americans are beginning to understand just how she felt. As reading and writing, health care and

Software for Privacy Protection

Many of the privacy-protection

shopping and sex and gossip increasingly take place in cyberspace, it is suddenly dawning on us that the most intimate details of our daily lives are being monitored, searched, recorded and stored as meticulously as Monica Lewinsky's were. For most citizens, however, the greatest threat to privacy comes not from special prosecutors but from employers and from all-seeing Web sites and advertising networks that track every move we make in cyberspace.

Consider the case of DoubleClick Inc. For the past few years, DoubleClick, the Internet's largest advertising company, has been compiling detailed information on the browsing habits of millions of Web users by placing "cookie" files on our hard drives. Cookies are electronic footprints that allow Web sites and advertising networks to monitor our online movements with telescopic precision -- including the search terms we enter as well as the articles we skim and how long we spend skimming them. Once DoubleClick sends you a cookie, you will receive targeted ads when you visit the Web sites of its 2,500 clients. So, for example, if you visit Alta Vista's auto section you may be greeted by a cheerful ad from G.M. or Ford.

As long as users were confident that their virtual identities weren't being linked to their actual identities, many were happy to accept DoubleClick cookies in exchange for the convenience of navigating the Web more efficiently. Then last November, DoubleClick bought Abacus Direct, a database of names, addresses and information about off-line buying habits of 90 million households, compiled from the largest direct mail catalogs and retailers in the nation. In January, DoubleClick began compiling profiles linking individuals' actual names and addresses to Abacus's detailed records of their online and off-line purchases. Suddenly, shopping that once seemed anonymous was being archived in personally identifiable dossiers.

Under pressure from privacy advocates and from dot-com investors, DoubleClick announced in March that it would postpone its profiling scheme until the federal government and the e-commerce industry agree on privacy standards. Still, the DoubleClick controversy points to the inherent threat

---

Jeffrey Rosen is an associate professor at the George Washington University Law School and the legal affairs editor of The New Republic. This article is adapted from his book, "The Unwanted Gaze: The Destruction of Privacy in

software programs discussed in this article can be downloaded. Here's a sampling:

•Freedom 1.1, a privacy program that uses online pseudonyms and cryptography to provide internet security.

•ZipLip, a program that encrypts and "shreds" electronic mail.

•Kremlin, a file-encryption program for Macintosh computers.

Note: The above links should not be construed as an endorsement of these companies' products or services. These sites are not part of The New York Times on the Web, and The Times has no control over their content or availability.

America." to be published next month by Random House.

to privacy in a new economy that is based, in unprecedented ways, on the recording and exchange of intimate personal information. Privacy protects us from being misdefined and judged out of context. This protection is especially important in a world of short attention spans, a world in which information can easily be confused with knowledge. When intimate personal information circulates among a small group of people who know you well, its significance can be weighed against other aspects of your personality and character. (Monica Lewinsky didn't mind that her friends knew she had given the president a copy of Nicholson Baker's "Vox" because her friends knew that she was much more than a person who would read a book about phone sex.) But when your browsing habits -- or e-mail messages -- are exposed to strangers, you may be reduced, in their eyes, to nothing more than the most salacious book you once read or the most vulgar joke you once told. And even if your Internet browsing isn't in any way embarrassing, you run the risk of being stereotyped as the kind of person who would read a particular book or listen to a particular song. Your public identity may be distorted by fragments of information that have little to do with how you define yourself. In a world where citizens are bombarded with information, people form impressions quickly, based on sound bites, and these brief impressions tend to oversimplify and misrepresent our complicated and often contradictory characters.

The sociologist Georg Simmel observed nearly 100 years ago that people are often more comfortable confiding in strangers than in friends, colleagues or neighbors. Confessions to strangers are cost-free because strangers move on; you never expect to see them again, so you are not inhibited by embarrassment or shame. In many ways the Internet is a technological manifestation of the phenomenon of the stranger. There's no reason to fear the disclosure of intimate information to faceless Web sites as long as those Web sites have no motive or ability to collate the data into a personally identifiable profile that could be disclosed to anyone you actually know. By contrast, the prospect that your real identity might be linked to permanent databases of your online -- and off-line -- behavior is chilling, because the databases could be bought, subpoenaed or traded by employers, insurance companies, ex-spouses and others who have the ability to affect your life in profound ways.

The retreat of DoubleClick may seem like a victory for privacy, but it is only an early battle in a much larger war -- one in which many expect privacy to be vanquished. "You already have zero privacy -- get over it," Scott McNealy, the C.E.O. of Sun Microsystems, memorably remarked

Ask the Author

Is It Safe to Be Yourself?
In the intimate and supposedly anonymous online world, people reveal their private selves with each click, purchase and message. As technology

makes our online selves more visible, is it important, or even possible, to protect privacy in cyberspace?

Post your comments and questions for Jeffrey Rosen, author of "The Unwanted Gaze," and read his responses this week.

last year in response to a question at a product show introducing a new interactive technology called Jini. Sun's cheerful Web site promises to usher in the "networked home" of the future, in which the company's "gateway" software will operate "like a congenial party host inside the home to help consumer appliances communicate intelligently with each other and with outside networks." In this chatty new world of electronic networking, your refrigerator and coffee maker can talk to your television, and all can be monitored from your office computer. The incessant information exchanged by these gossiping appliances might, of course, generate detailed records of the most intimate details of your daily life. Your liquor cabinet might tell Pinkdot.com, the online grocer, that you are low on whiskey, prompting your television to start blaring ads for alcoholics anonymous. But this may not be what Sun Microsystems has in mind when it boasts about the pleasures of the "connected family."

New evidence seems to emerge every day to support McNealy's grim verdict about the triumph of online surveillance technology over privacy. A former colleague of mine who runs a Web site for political junkies recently sent me the "data trail" statistics that he receives each week. They disclose not only the Internet addresses of individual browsers who visit his site, clearly identifying their universities or corporate employers, but also the Web sites each user visited previously and the articles he or she downloaded there. And it's increasingly common to find programs in the workplace that report back to a central server all the Internet addresses that employees visit. After the respected dean of the Harvard Divinity School was forced to step down in 1998 for downloading pornography on his home computer, a former Harvard computer technician wrote an article for Salon, the online magazine, criticizing his former colleagues for snitching on the dean. "In the server room of one of my part-time jobs," the techie confessed, "I noticed that a program called Gatekeeper displayed all the Internet usage in the office as it happened. I sat and watched people send e-mail, buy and sell stocks on e-trade and download pictures of Celine Dion. If I had wanted I could have traced this usage back to the individual user."

A survey of nearly a thousand large companies conducted last year by the American Management Association found that 45 percent monitored the e-mail, computer files or phone calls of their workers, up from 35 percent two years earlier. Some companies use Orwellian computer software with names like Spector, Assentor or Investigator, available for as little as $99, that can monitor and record every keystroke on the computer with videolike precision. These virtual snoops can also be programmed to screen all incoming

and outgoing e-mail for forbidden words and phrases -- involving racism, body parts or the name of your boss -- and can forward suspicious messages to a supervisor for review. E-mail can be resurrected from computer hard drives even after it has ostensibly been deleted. And companies are increasingly monitoring jokes and e-mail sent from home as well as work over company servers.

The most common justification for Internet and e-mail monitoring in the workplace is fear of liability under sexual harassment law, which requires companies to protect workers from speech that might be construed to create a "hostile or offensive working environment." Because employers cannot be sure in advance what sort of e-mail or Web browsing a particular employee might find offensive, they have an incentive to monitor far more Internet activity than the law actually forbids.

Changes in the delivery of books, music and television are extending these technologies of surveillance beyond the office, blurring the boundaries between work and home. Last summer, for example, Amazon.com was criticized for a feature that uses ZIP codes and domain names to identify the most popular books purchased online by employees at prominent corporations. (The top choice at Charles Schwab: "Memoirs of a Geisha.") And anonymous browsing continues to be under assault. The Sprint wireless Web phone that I bought in March promptly revealed my new telephone number to Amazon's pre-programmed Web site when I dialed in the hope of browsing discreetly for ordering information about my new book.

The same technologies that are making it possible to download digitally stored books, CD's and movies directly onto our hard drives will soon make it possible for publishers and entertainment companies to record and monitor our browsing habits with unsettling specificity. "Snitchware" programs can regulate not only which books you read but also how many times you read them, charging different royalties based on whether you copy from the book or forward part of it to a friend. Television, too, is being redesigned to create precise records of our viewing habits. A new electronic device known as a personal video recorder makes it possible to store up to 30 hours of television programs; it also enables viewers to skip commercials and to create their own lineups. One of the current models, TiVo, establishes viewer profiles that it then uses to make viewing suggestions and to record future shows. And in a world where media conglomerates like AOL-Time Warner can monitor your activities in cyberspace and then use your

browsing habits to determine the content that is beamed to you through television, books, movies and magazines, the integrated media box of the future may have surveillance capabilities that make DoubleClick's database look benign.

As if that weren't bad enough, Globally Unique Identifiers, or GUID's, are making it possible to link every document you create, message you e-mail and chat you post with your real-world identity. GUID's are a kind of serial number that can be linked with your name and e-mail address when you register online for a product or service. Last November, RealJukebox, one of the most popular Internet music players, with 30 million registered users, became a focus of media attention when privacy advocates noted that the player could relay information to its parent company, RealNetworks, about the music each user downloaded, and that this could be matched with a unique ID number that pinpointed the user's identity. At a conference about privacy in cyberspace held at the Stanford Law School in February, a lawyer for RealNetwork, Bob Kimball, insisted that the company had never, in fact, matched the GUID's with the data about music preferences. Nevertheless, hours after the media outcry began, RealNetworks disabled the GUID's to avoid a DoubleClick-like public relations debacle. But some currently available software products, like Microsoft's Word 97 and Powerpoint 97, embed unique identifiers into every document. Soon, all electronic documents created electronically may have invisible markings that could be traced back to the author or recipient.

There is nothing new about the fear that new technologies of surveillance and communication are altering the nature of privacy. A hundred years ago, in the most famous essay on privacy ever written, Louis D. Brandeis and Samuel Warren worried that new media technologies -- in particular the invention of instant photographs and the tabloid press -- were invading "the sacred precincts of private and domestic life." What outraged Brandeis and Warren was a mild society item in The Boston Saturday Evening Gazette that described a lavish breakfast party that Warren himself had put on for his daughter's wedding. Although the information itself wasn't inherently salacious, Brandeis and Warren were appalled that a domestic ceremony would be described in a gossip column and discussed by strangers.

At the beginning of the 21st century, however, the Internet has vastly expanded the aspects of private life that can be monitored and recorded. As a result, cyberspace has increased the danger that personal information originally disclosed to friends and colleagues may be exposed to, and misinterpreted by, a less-understanding audience. Gossip that in Brandeis and Warren's day might have taken place in a drawing room is now recorded in a chat room and can be retrieved years later anywhere on earth. Several months ago, The Washington Post, for example, described the case of James

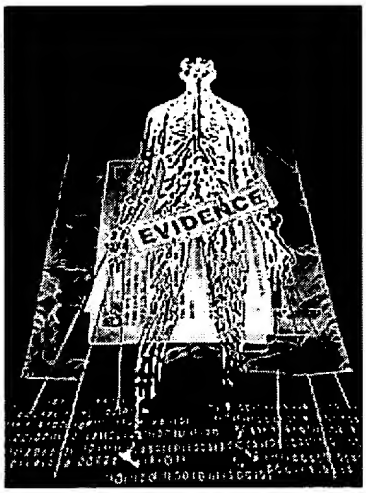
Rutt, a man who worried that his Internet past might be misconstrued if taken out of context.

Even when employers promise to respect the privacy of e-mail, courts are upholding their right to break promises without warning.

Rutt had spent years unburdening himself in a chat group. Although he had been happy to speak candidly in the sympathetic confines of a space characterized as "a virtual corner bar," once he was appointed to a new position as C.E.O. of Network Solutions Inc., he feared that his musings about sex, politics and his own weight problem might embarrass him, or worse. Fortunately for Rutt, the chat group offered a special software feature called Scribble that allowed him to erase a decade of his own postings. But as intimate information about our lives is increasingly recorded, archived and not easily deleted, there is a growing danger that a part of our identities will come to be mistaken for who we are. In certain circles today it is not uncommon for prospective romantic partners, before going out on dates, to perform background checks on each other, scouring the Internet for as much personal information as possible. And these searches can be a deal-breaker: a friend of mine, after being set up on a blind date, ran an Internet search and discovered that her prospective partner had been described in an article for an online magazine as one of the 10 worst dates of all time; the article included intimate details about his sexual equipment and performance that she was unable to banish from her mind during their first -- and only -- dinner. These are the sort of details, of course, that friends often exchange in informal gossip networks. The difference now is that the most intimate personal information is often recorded indelibly and can be retrieved with chilling efficiency by strangers around the globe.

In a famous essay on reputation published in 1890, E.L. Godkin, the editor of the Nation, elaborated on the distinction between oral and written gossip. As long as gossip was oral, and circulated among acquaintances rather than strangers, Godkin wrote, its objects were often spared the mortification of knowing they were being gossiped about. Oral gossip is a flexible way of enforcing communal norms while still respecting privacy. When neighbors gossip about one anothers' intimate activities, those who behave badly will soon feel the indirect effects of social disapproval. The wrongdoers can then correct their misbehavior without feeling that their public faces have been assaulted. And because all of the relevant parties know one another well based on close personal observation, individual transgressions can be weighed against the broader picture of an individual's personality.

Cyberspace, however, has blurred the distinction between oral and written



gossip by recording and publishing the kind of private information that used to be exchanged around the water cooler. Unlike oral gossip, Internet gossip is hard to answer, because its potential audience is anonymous and unbounded. A Web site called Disgruntled Housewife (www.disgruntledhousewife.com) offers an appalling feature called the Dick List, designed to promote "girly solidarity through bile-spewing," in which women from around the country write in to describe the most intimate secrets of former lovers they dislike. (The men are identified by their home towns and sometimes by their full names, a few letters of which are fatuously omitted.) Furthermore, when the gossip is archived, it can come back to haunt. If, in a moment of youthful enthusiasm, I posted intemperate comments to an Internet newsgroup, those comments could be retrieved years later simply by typing my name or Internet protocol address into a popular search engine. For more and more citizens the most important way of exchanging gossip is e-mail. But instead of giving private e-mail the same legal protections as private letters, courts are increasingly treating e-mail as if it were no more private than a postcard. In an entirely circular legal test, the Supreme Court has held that constitutional protections against unreasonable searches depend on whether citizens have subjective expectations of privacy that society is prepared to accept as reasonable. This means that as technologies of surveillance and data collection have become ever more intrusive, expectations of privacy have naturally diminished, with a corresponding reduction in constitutional protections. More recently, courts have held that merely by adopting a written policy that warns employees that their e-mail may be monitored, employers will lower expectations of privacy in a way that gives them virtually unlimited discretion to monitor e-mail.

Even when employers promise to respect the privacy of e-mail, courts are upholding their right to break their promises without warning. A few years ago in a case in Pennsylvania, the Pillsbury Company repeatedly promised its employees that all e-mail would remain confidential and that no employee would be fired based on intercepted e-mail. Michael Smyth, a Pillsbury employee, received an e-mail message from his supervisor over the company's computer network, which he read at home. Relying on the company's promise about the privacy of e-mail, he sent an intemperate reply to the supervisor, supposedly saying at one point that he felt like killing "the backstabbing bastards" on the sales force, and referring to a holiday party as the "Jim Jones Koolaid affair."

Despite the company's promises, it proceeded to retrieve from its

computers dozens of e-mail messages that Smyth had sent and received, and then fired him for transmitting "inappropriate and unprofessional comments." Smyth sued, arguing that the company had invaded his right to privacy by firing him. But the court blithely dismissed his claim on the grounds that Pillsbury owned the computer system and therefore could intercept e-mail sent from home or work without invading its workers' legitimate expectations of privacy.

This can't be right. I'm at home as I type these words, but the computer on which I'm typing is owned by the law school I teach at, as is the network that supplies my e-mail access. I would be appalled if anyone suggested that the provision of these research tools gave my law school the right to monitor all the e-mail I send and receive. In 1877, the Supreme Court held that postal inspectors need a search warrant to open first-class mail, regardless of whether it is sent from the office or from home. And searches of e-mail can be even more invasive than searches of written letters. Georg Simmel wrote about the ways in which written letters are peculiarly subject to misinterpretation. Because letters lack the contextual accompaniments -- sound of voice, tone, gesture, facial expression" -- that, in spoken conversation, are a source of obfuscation and clarification, Simmel argued, letters can be more easily misinterpreted than speech. With e-mail, the possibilities for misinterpretation are even more acute. E-mail combines the intimacy of the telephone with the infinite retrievability of a letter. And because e-mail messages are often dashed off quickly, they may, when taken out of context, provide an inaccurate window onto someone's emotions. In 1997, for example, Judge Thomas Penfield Jackson chose Lawrence Lessig of Harvard Law School to advise him in overseeing the antitrust dispute between the government and Microsoft. When Microsoft challenged Lessig's appointment as a "special master," Netscape officials turned over to the Justice Department an e-mail message that Lessig had written to an acquaintance at Netscape in which he joked that he had "sold my soul" by downloading Microsoft's Internet Explorer. The Justice Department, in turn, gave Lessig's e-mail to Microsoft, which claimed he was biased and demanded his resignation.

Cyberspace has blurred the distinction between oral and written gossip by recording and publishing the kind of private information that

In fact, Lessig's e-mail had been quoted out of context. As the full text of the e-mail makes clear, Lessig had downloaded Microsoft's Internet Explorer to enter a contest to win a PowerBook. After installing the Explorer, he discovered that his Netscape bookmarks had been erased. In a moment of frustration, he fired off the e-mail to the Netscape acquaintance, whom he had met at a cyberspace conference, describing what had happened and quoting a Jill Sobule song that had

used to be exchanged around the water cooler.

been playing on his car stereo: "Sold my soul, and nothing happened." And although a court ultimately required Lessig to step down as special master for technical reasons having nothing to do with his misinterpreted e-mail, he discovered that strangers were left with the erroneous impression that the e-mail "proved" that he was biased, and that it was this that brought about his resignation. The experience taught Lessig that, in a world where most electronic footsteps are recorded and all records can be instantly retrieved, it is very easy for sentiments to be taken out of their original context by people who want to do someone ill.

"The thing I felt most about the Microsoft case was not the actual invasion (as I said, I didn't really consider it much of an invasion)," Lessig wrote in an e-mail message to me after the ordeal. "What I hated most was that the issue was just not important enough for people to understand enough to understand the truth. It deserved one second of the nation's attention, but to understand the issue would have required at least a minute's consideration. But I didn't get, and didn't deserve, a minute's consideration. Thus, for most, the truth was lost." Lessig felt ill treated, in short, not because he wasn't able to explain himself, but because, in a world of short attention spans, he was never given the chance. In what might be seen as poetic justice, Microsoft itself was embarrassed in the antitrust trial that followed when e-mail from top executives, from Bill Gates on down, was turned over to the government and introduced in court.

Unchastened by Lessig's experience, I behave as if my online life isn't virtually transparent, even though I understand on some level that it is. Not long ago, I visited my law school's computer center to find out how many of my online activities were in fact being monitored. "If I happen to be in the server room, I can watch you send e-mail, and I'll know who you're sending it to," said the discreet head of the center. Beyond that, I was pleased to learn, the law school has decided not to install the programs that many companies use to monitor the browsing, reading and writing of their employees in real time, or to make regular copies of hard drives, including the cache files that record all the Internet documents a user has downloaded. But if I, like the former dean of Harvard Divinity School, asked school technicians to repair my home computer, the school would be able to reconstruct my personal and professional online activities with granular precision.

Perhaps the only sane response to the new technologies of surveillance in cyberspace is unapologetic paranoia. If so, my candidate for the perfectly rational man is K., one of my former students. K. wears green Army fatigues and black boots and spends much of his day shredding and covering his electronic tracks. "In my home office, I have five computers with AtGuard personal firewalls," he explained to me not long ago. "With AtGuard you can

monitor how many backdoors you have open to the Internet, so if someone is spying on you with a hacking program like BackOrifice or NetBus, you can kill that connection." Whenever an uninvited Web site tries to send K. a cookie, AtGuard fires back a cookie that says, "Keep your cookies off my hard drive." Aware that files and e-mail can be resurrected from his hard drive even after they are ostensibly deleted, K. also uses a suite of security tools called Kremlin. Every time K. turns off his computer, Kremlin does a "secure total wipe" of his 20 gigabyte hard drive, scribbling electronic graffiti, in the form of zeroes and ones, over all the free space so that any lurking, partly deleted files will be rendered illegible. This takes more than an hour. K. also uses Kremlin to encrypt his personal documents in a secure folder on his hard drive, and he carefully chose a nonsense password, garbled with upper- and lowercase letters and numbers, so that it can't easily be cracked by a "brute force attack program" that might hypothetically bombard his computer with millions of random words generated from an electronic dictionary. Impressed by his vigilance, I asked K. what, precisely, he was trying to hide. "It's more an ideological act than anything else," he said. "I know that I can be surveilled at all times, so I feel like I have a responsibility to resist."

Not everyone agrees that there is reason to resist the brave new world of virtual exposure. This is, after all, an exhibitionistic culture in which people cheerfully enact the most intimate moments of their daily lives on Web cams and on Fox TV. It is a culture in which Wesleyan students are offered a chance to live in a "naked" dorm and in which 2,000 confessional souls have chosen to post their most private thoughts on a site called Diarist.net, which boasts, "We've got everything you need to know all about the people who tell all." Defenders of transparency argue that there's no reason to worry about privacy if you have nothing to hide, and that more information, rather than less, is the best way to protect us against being judged out of context. We might think differently about a Charles Schwab employee who ordered "Memoirs of a Geisha" from Amazon.com, for example, if we knew that she also listened to the Doors and subscribed to Popular Mechanics.

But the defenders of transparency are confusing secrecy with privacy, and secrecy is only a small dimension of privacy. Even if we saw an Amazon.com profile of everything the Charles Schwab employee had read and downloaded this week, we wouldn't come close to knowing who she really is. (Instead, we would misjudge her in all sorts of new ways.) In a surreal world where complete logs of every citizen's reading habits were available on the Internet, the limits of other citizens' attention spans would guarantee that no one could focus long enough to read someone else's browsing logs from beginning to end. Instead, overwhelmed by information, citizens would change the channel or click to a more interesting Web site.

Even the most sophisticated surveillance technologies can't begin to

absorb, analyze and understand the sheer volume of information. The F.B.I. recently asked Congress for $75 million to finance a series of surveillance systems,including a new project called Digital Storm, which will allow it to vastly expand its recordings of foreign and domestic telephone and cell-phone calls, after receiving judicial authorization.

But because it can't possibly hire enough agents to listen to the recordings from beginning to end, the F.B.I. plans to use "data mining" technology to search for suspicious key words. This greatly increases the risk that information will be taken out of context: as "60 Minutes" reported, the Canadian Security Agency identified a mother as a potential terrorist after she told a friend on the phone that her son had "bombed" in his school play. Filtered or unfiltered, information taken out of context is no substitute for the genuine knowledge that can emerge only slowly over time.

Moreover, defenders of transparency have adopted a unified vision of human personality, which views social masks as a way of misrepresenting the true self. But as the sociologist Erving Goffman argued in the 1960's, this take on personality is simplistic and misleading. Instead of behaving in a way that is consistent with a single character, people reveal different parts of themselves in different contexts. I may -- and do -- wear different social masks when interacting with my students, my editors, my colleagues and my dry cleaner. Far from being inauthentic, each of these masks helps me try to behave in a manner that is appropriate to the different roles demanded by these different social settings. If these masks were to be violently torn away, what would be exposed is not my true self but the spectacle of a wounded and defenseless man.

Goffman also maintained that individuals, like actors in a theater, need backstage areas where they can let down their public masks, tell dirty jokes, collect themselves and relieve the tensions that are an inevitable part of public performance. In the new economy of information exchange, white collar workers are increasingly forced to work under constant surveillance like the dehumanized hero of "The Truman Show," a character who has been placed on an elaborate stage set without his knowledge or consent and whose every move, as he interacts with the actors who have been hired to play his friends and family, is broadcast by hidden video cameras.

The inhibiting effects on creativity and efficiency are palpable. Surveys of the health consequences of monitoring in the workplace have suggested that electronically monitored workers experience higher levels of depression, tension and anxiety and lower levels of productivity than those who are not monitored. Unsure about when, precisely, electronic monitoring may take place, employees will necessarily be far more guarded and less spontaneous, and the increased formality of conversation and e-mail can make communication less efficient. Moreover, spying on people without

their knowledge is an indignity. It fails to treat its objects as fully deserving of respect, and treats them instead like animals in a zoo, deceiving them about the nature of their own surroundings.

In "The Unbearable Lightness of Being," Milan Kundera describes how the police destroyed an important figure of the Prague Spring by recording his conversations with a friend and then broadcasting them as a radio serial. Reflecting on his novel in an essay on privacy, Kundera writes, "Instantly Prochazka was discredited: because in private, a person says all sorts of things, slurs friends, uses coarse language, acts silly, tells dirty jokes, repeats himself, makes a companion laugh by shocking him with outrageous talk, floats heretical ideas he'd never admit in public and so forth." Freedom is impossible in a society that refuses to respect the fact that "we act different in private than in public," Kundera argues, a reality that he calls "the very ground of the life of the individual." By requiring citizens to live in glass houses without curtains, totalitarian societies deny their status as individuals, and "this transformation of a man from subject to object is experienced as shame."

A liberal state should respect the distinction between public and private speech because it recognizes that the ability to expose in some contexts aspects of our identity that we conceal in other contexts is indispensable to freedom, friendship, even love. Friendship and romantic love can't be achieved without intimacy, and intimacy, in turn, depends upon the selective and voluntary disclosure of personal information that we don't share with everyone else. Moreover, as Kundera recognized, privacy is also necessary for the development of human individuality. Any writer will understand the importance of reflective solitude in refining arguments and making unexpected connections: in an odd but widely shared experience, many of us seem to have our best ideas when we are in the shower. Indeed, studies of creativity show that it's during periods of daydreaming and seclusion that the most creative thought takes place, as individuals allow ideas and impressions to run freely through their minds without fear that their untested thoughts will be exposed and taken out of context.

It is surprising how recently changes in law and technology have been permitted to undermine sanctuaries of privacy that Americans have long taken for granted. But even more surprising has been our relatively tepid response to the new technologies of exposure. But there is no reason to surrender to technological determinism; no reason to accept the smug conclusion of Silicon Valley that in the war between privacy and technology, privacy is doomed. On the contrary, there is a range of technological, legal and political responses that might help us rebuild in cyberspace some of the privacy and anonymity that we demand in real space.

The most effective responses may be forms of self-help that allow

citizens to cover their electronic tracks, along the lines of the Kremlin technology that my student uses to scour his hard drive or the Scribble technology that James Rutt used to erase his own chat. The fact that e- mail, for example, is hard to delete and easy to retrieve is partly a consequence of current technology, and technology can change. Companies with names like Disappearing Inc. and ZipLip have introduced a form of self-deleting e-mail that uses encryption technology to make messages nearly impossible to read soon after they are received. When I send you a message, Disappearing Inc. scrambles the e-mail with an encrypted key and then gives you the same key to unscramble it. I can specify how long I want the key to exist, and after the key is destroyed, the message can't be read without a herculean code-breaking effort.

At the moment the most advanced technology of anonymity and pseudonymity in cyberspace is offered by companies like Zero-Knowledge Systems, which is based in Montreal. For a modest fee, you can disaggregate your identity with a software package called Freedom, which initially gives you five digital pseudonyms, or "nyms," that you can assign to different activities, from discussing politics to surfing the Web. (Why any of us needs five pseudonyms isn't entirely clear, but the enthusiasm of the privacy idealists is sweet in its way.) On the Freedom system, no one, not even Zero-Knowledge itself, can trace your pseudonyms back to your actual identity.

"You can trust us because we're not asking you to trust us," says Austin Hill, Zero-Knowledge's 26-year-old president. Hill has a messianic air about his role in vindicating what he considers to be the universal human rights of privacy, free speech and the possibility of redemption in a world where youthful errors can follow you for the rest of your life. "Twenty years from now, I'm going to be able to talk to my grandkids and say I played an instrumental role in making the world a better place," he says. "As the Blues Brothers say, everyone here feels that we're on a mission from God."

Freedom makes traceability difficult by encrypting e-mail and Web-browsing requests and sending them through at least three intermediary routers on the way to their final destinations: each message is wrapped like an onion in three layers of cryptography, and each router can peel off only one layer of the onion to learn the next stop in the path of the message. Because no single router knows both the source of the message and its destination, the identity of the sender and the recipient is difficult to link. Zero-Knowledge assigns pseudonyms using the same technology, and so the company itself can't link the pseudonyms to individual users; if it is subpoenaed it can only turn over a list of its customers, who can hope for anonymity in numbers.

But should people be forced to resort to esoteric encryption

technology with names like ZipLip and Zero-Knowledge every time they want to send e-mail or browse the Web? Until anonymous browsers become widespread enough to be socially acceptable, their Austin Powers-like aura may deter all but the most secretive users who have something serious to hide. Moreover, every technological advance for privacy will eventually provoke a technological response. For this reason, some privacy advocates, like Marc Rotenberg, the director of the Electronic Privacy Information Center, argue that anonymity on the Internet should be a legal right, rather than something achieved with a commercial product.

The battle for privacy must be fought on many fronts - legal, political and technological - and each new assault must be vigilantly resisted as it occurs.

Americans increasingly seem to agree that Congress should save us from the worst excesses of online profiling. In a Business Week poll conducted in March, 57 percent of the respondents said that the government should pass laws regulating how personal information can be collected and used on the Internet. The European Union for example, has adopted the principle that information gathered for one purpose can't be sold or disclosed for another purpose without the consent of the individual concerned. But efforts to pass comprehensive privacy legislation in the United States have long been thwarted by a political reality: the beneficiaries of privacy -- all of us, in the abstract -- are anonymous and diffuse, while the corporate opponents of privacy are well organized and well heeled.

In the hope that the political tide may be turning, Senator Robert Torricelli has introduced a bill that would forbid a Web site from collecting or selling personal data unless users checked a box allowing it to do so. This "opt in" proposal has been vigorously and successfully resisted by the e-commerce lobby, which insists that it would cripple the use of online profiling and cause advertising revenues to plummet.

The e-commerce lobby prefers a more modest Senate proposal that would require Web sites to display a clearly marked box allowing users to "opt out" of data collection and resale. But it's not clear that "opt out" proposals would provide meaningful protection for privacy. Many users, when confronted with boilerplate privacy policies, tend to click past them as quickly as teenage boys click past the age certification screens on X-rated Web sites.

Moreover, many people seem happy to waive their privacy rights in exchange for free stuff. There is now a cottage industry of companies with names like Free PC, Dash.com and Gator.com that offer their users product discounts, giveaways or even cash in

exchange for permission to track, record and profile every move they make, and to bombard them with targeted ads on the basis of their proclivities.

This is about as rational as allowing a camera into your bedroom in exchange for a free toaster. But as Monica Lewinsky discovered, it's easy to forget why privacy is important until information you care about is taken out of context, and by that point, it's usually too late. "One of the things that I was a little bit disappointed about," Lewinsky told Larry King, "was that people didn't seem to pay too much attention about their privacy issues." In what will hopefully be the last indignity for Lewinsky, some of her previously undiscovered e-mail messages to Betty Currie surfaced only a few weeks ago, when the White House turned them over in response to a subpoena in an unrelated case. In cyberspace, as in cheap horror movies, your ghosts can rise up to haunt you just when you think the danger has passed.

There is no single solution to the erosion of privacy in cyberspace: no single law that can be proposed or single technology that can be invented to stop the profilers and surveillants in their tracks. The battle for privacy must be fought on many fronts -- legal, political and technological -- and each

new assault must be vigilantly resisted as it occurs. But the history of political responses to new technologies of surveillance provides some grounds for hope. Although Americans are seldom roused to defend privacy in the abstract, the most illiberal and intrusive technologies of surveillance have, in fact, provoked political outrage that has forced the data collectors to retreat. In 1967, after the federal government proposed to create a national data center that would store personal information from the I.R.S., the census and labor bureaus and the Social Security administration, Vance Packard wrote an influential article for this magazine that helped to kill the plan.

We are trained in this country to think of all concealment as a form of hypocrisy. But perhaps we are about to learn how much may be lost in a culture of transparency -- the capacity for creativity and eccentricity, for the development of self and soul, for understanding, friendship and even love. There is nothing inevitable about the erosion of privacy in cyberspace, just as there is nothing inevitable about its reconstruction. We have the ability to rebuild some of the private spaces we have lost. What we need now is the will.

Table of Contents
April 30, 2000